

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 18 FEB 2000

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 2月 8日

出願番号

Application Number:

平成11年特許願第030600号

出願人

Applicant(s):

ソニー株式会社

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN

COMPLIANCE WITH

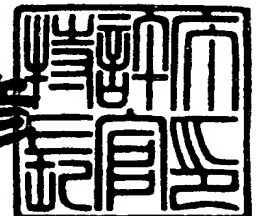
RULE 17.1(a) OR (b)

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年12月24日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特平11-3091180

【書類名】 特許願

【整理番号】 9900070509

【提出日】 平成11年 2月 8日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 7/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 浅野 智之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 大澤 義知

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録／再生システム、情報記録装置、情報再生装置、認証データ記録装置、情報記録媒体、認証データの記録方法、情報記録媒体の認証方法、情報記録方法及び情報再生方法

【特許請求の範囲】

【請求項 1】 情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録装置と、

上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行い、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体を介して記録／再生する情報記録／再生装置と

からなる情報記録／再生システム。

【請求項 2】 上記認証データ記録装置は、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 3】 上記情報記録／再生装置は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記ユーザデータの暗号化に用いる暗号鍵を暗号化し、上記暗号鍵により暗号化したユーザデータと上記暗号化した暗号鍵を上記認証された情報記録媒体を介して記録／再生することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項4】 上記情報記録／再生装置は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記ユーザデータの暗号化に用いる暗号鍵を生成することを特徴とする請求項3記載の情報記録／再生システム。

【請求項5】 ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体にユーザデータを記録する情報記録装置であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、

上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、

情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、

上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、上記暗号鍵と暗号化したユーザデータを上記認証された情報記録媒体に記録する記録手段と

を備えることを特徴とする情報記録装置。

【請求項6】 上記認証処理手段は、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項5記載の情報記録装置。

【請求項7】 上記認証処理手段は、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求

項 5 記載の情報記録装置。

【請求項 8】 上記認証処理手段は、上記リボケーションリストを格納する記憶手段を有し、情報記録媒体に記録されていたリボケーションリストが正当なものであり、上記記憶手段に格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを上記記憶手段に格納し、上記記憶手段に格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 7 記載の情報記録装置。

【請求項 9】 上記記録手段は、暗号鍵を生成する暗号鍵生成手段と、上記媒体識別情報を用いて上記暗号鍵を暗号化する暗号鍵暗号化手段と、上記暗号鍵を用いてユーザデータを暗号化するユーザデータ暗号化手段とを備え、

上記ユーザデータ暗号化手段により暗号化したユーザデータと上記暗号鍵暗号化手段により暗号化した暗号鍵を上記認証された情報記録媒体に記録することを特徴とする請求項 5 記載の情報記録装置。

【請求項 10】 上記暗号鍵生成手段は、上記媒体識別情報を用いて暗号鍵を生成することを特徴とする請求項 9 記載の情報記録装置。

【請求項 11】 ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体からユーザデータを再生する情報再生装置であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、

上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、

情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、

上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて暗号

鍵を生成する暗号鍵生成手段と、

上記暗号鍵生成手段により生成された暗号鍵を用いてユーザデータを復号する復号手段を備え、

上記認証処理手段により認証された情報記録媒体上のユーザデータ記録部から、上記媒体識別情報を用いて生成された暗号鍵により暗号化されたユーザデータを上記復号手段により復号して再生することを特徴とする情報再生装置。

【請求項 12】 上記認証処理手段は、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項 11 記載の情報再生装置。

【請求項 13】 上記認証処理手段は、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 12 記載の情報再生装置。

【請求項 14】 上記認証処理手段は、上記リボケーションリストを格納する記憶手段を有し、情報記録媒体に記録されていたリボケーションリストが正当なものであり、上記記憶手段に格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを上記記憶手段に格納し、上記記憶手段に格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 11 記載の情報再生装置。

【請求項 15】 ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出手段と、

上記ランダムパターン情報検出手段により検出された上記ランダムパターン情

報から媒体識別情報を生成する媒体識別情報生成手段と、

上記媒体識別情報生成手段により生成した媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録手段と

を備えることを特徴とする認証データ記録装置。

【請求項 16】 上記認証データ記録手段は、上記認証データ記録部に製造者についてのリボケーションリストを上記認証データとともに記録することを特徴とする請求項 15 記載の認証データ記録装置。

【請求項 17】 ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部と、

上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部と、

ユーザデータが記録されるユーザデータ記録部と

を有することを特徴とする情報記録媒体。

【請求項 18】 上記認証データ記録部に製造者についてのリボケーションリストが上記認証データとともに記録されたことを特徴とする請求項 17 記載の情報記録媒体。

【請求項 19】 情報記録媒体に記録されたランダムな物理現象によるランダムパターン情報を検出し、

上記ランダムパターン情報から媒体識別情報を生成し、

上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体に記録する

ことを特徴とする認証データの記録方法。

【請求項 20】 製造者についてのリボケーションリストを上記認証データとともに上記情報記録媒体に記録することを特徴とする請求項 19 記載の認証データの記録方法。

【請求項 21】 情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が該媒体識別情報に対する製造者

毎のデジタル署名とともに認証データとして記録された情報記録媒体から、

上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、

上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて、上記情報記録媒体の認証処理を行う

ことを特徴とする情報記録媒体の認証方法。

【請求項 22】 製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、

上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、正当なデジタル署名に基づいて認証処理を行う

ことを特徴とする請求項 21 記載の情報記録媒体の認証方法。

【請求項 23】 製造者についてのリボケーションリストを記憶しておき、情報記録媒体に記録されていたリボケーションリストが正当なものであり、先に記憶したリボケーションリストよりも新しい場合に、記憶していたリボケーションリストを更新し、

最新のリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 21 記載の情報記録媒体の認証方法。

【請求項 24】 扱った情報記録媒体の製造者の識別情報とその公開鍵をリボケーションフラグとともに記憶して記憶しておき、新しいリボケーションリストを用いてリボケーションフラグを更新し、

リボケーションフラグを用いて上記認証データに含まれるデジタル署名の正当性を検証し、正当なデジタル署名に基づいて認証処理を行う

ことを特徴とする請求項 21 記載の情報記録媒体の認証方法。

【請求項 25】 情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、

上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情

報検査データを生成するとともに、

上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、

上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、

上記暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体に記録することを特徴とする情報記録方法。

【請求項 26】 暗号鍵によりユーザデータを暗号化するとともに、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて上記暗号鍵を暗号化し、

上記暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体に記録することを特徴とする請求項 25 記載の情報記録方法。

【請求項 27】 上記媒体識別情報を用いて暗号鍵を生成し、上記暗号鍵によりユーザデータを暗号化することを特徴とする請求項 26 記載の情報記録方法。

【請求項 28】 上記認証処理では、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、検証された正当な媒体識別情報と上記媒体識別情報検査データに基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項 25 記載の情報記録方法。

【請求項 29】 上記認証処理では、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 25 記載の情報記録方法。

【請求項 30】 上記認証処理では、情報記録媒体に記録されていたリボケーションリストが正当なものであり、格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを新た

に格納し、格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 29 記載の情報記録方法。

【請求項 31】 情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、

上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、

上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、

認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、

上記暗号鍵を用いてユーザデータを復号し、

上記認証された情報記録媒体から上記暗号鍵を用いてユーザデータを復号することを特徴とする情報再生方法。

【請求項 32】 上記認証処理では、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、検証された正当な媒体識別情報と上記媒体識別情報検査データに基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項 31 記載の情報再生方法。

【請求項 33】 上記認証処理では、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 31 記載の情報再生方法。

【請求項 34】 上記認証処理では、情報記録媒体に記録されていたリボケーションリストが正当なものであり、格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを新た

に格納し、格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項 33 記載の情報再生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、RAMメディアに対する不正コピーを防止するようにした情報記録／再生システム、情報記録装置、情報再生装置、認証データ記録装置、情報記録媒体、認証データの記録方法、情報記録媒体の認証方法、情報記録方法及び情報再生方法に関する。

【0002】

【従来の技術】

近年、家庭内において音楽情報や映像情報などのデジタルデータを伝送したり記録したりする機器が広く普及している。これらの機器では、データを高品質で記録／再生することが可能であることから、何度複製しても品質劣化のない記録システムを構成することができる。このような記録システムでは、著作権のあるデータが不正にコピーされてしまうのを防止する著作権保護機能を装備する必要がある。

【0003】

このような著作権保護のためのシステムとして、例えば、Digital Video Disc (DVD) ROM におけるコンテンツスクランブルシステムがある。

【0004】

このシステムでは、ディスク上の著作権付きデータをすべて暗号化し、ライセンスを受けた機器だけが、暗号を復号して意味のあるデータを得るための暗号鍵を与えられるようにしている。ライセンスを受けた機器は、不正コピーを行わないなどの動作規定に従うように設計されている。

【0005】

【発明が解決しようとする課題】

しかし、上述の如きDVDシステムが採用している方式は、ROMメディアに

対して有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効でない。なぜならば、RAMメディアにおいては、不正者は、暗号を解読できないとしても、ディスク上のデータを全部、新しいディスクにコピーすることによって、正当な機器では動作してしまうディスクを新たに作ることができるからである。

【0006】

そこで、本発明の目的は、RAMメディアに対しても有効な不正コピー防止システムを構築した情報記録／再生システム、情報記録装置、情報再生装置、認証データ記録装置、情報記録媒体、認証データの記録方法、情報記録媒体の認証方法、情報記録方法及び情報再生方法を提供することにある。

【0007】

【課題を解決するための手段】

本発明に係る情報記録／再生システムは、情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録装置と、上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行い、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体を介して記録／再生する情報記録／再生装置とからなる。

【0008】

本発明に係る情報記録装置は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部

から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体にユーザデータを記録する情報記録装置であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、上記暗号鍵と暗号化したユーザデータを上記認証された情報記録媒体に記録する記録手段とを備えることを特徴とする。

【 0 0 0 9 】

本発明に係る情報再生装置は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体からユーザデータを再生する情報再生装置であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて暗号鍵を生成する暗号鍵生成手段と、上記暗号鍵生成手段により生成された暗号鍵を用いてユーザデータを復号する復号手段を備え、上記認証処理手段により認証された情報記録媒体上のユーザデータ記録部から、上記媒体識別情報を用いて生成された暗号鍵により暗号化されたユーザデータを上記復号手段により復号して再生することを特徴とする

【0010】

本発明に係る認証データ記録装置は、ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出手段と、上記ランダムパターン情報検出手段により検出された上記ランダムパターン情報から媒体識別情報を生成する媒体識別情報生成手段と、上記媒体識別情報生成手段により生成した媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録手段とを備えることを特徴とする。

【0011】

本発明に係る情報記録媒体は、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部と、ユーザデータが記録されるユーザデータ記録部とを有することを特徴とする。

【0012】

本発明に係る認証データの記録方法は、情報記録媒体に記録されたランダムな物理現象によるランダムパターン情報を検出し、上記ランダムパターン情報から媒体識別情報を生成し、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体に記録することを特徴とする。

【0013】

本発明に係る情報記録媒体の認証方法は、情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体から、上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて、上記情報記録媒体の認証処理を行うことを特徴とする。

【0014】

本発明に係る情報記録方法は、情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、上記暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体に記録することを特徴とする。

【0015】

本発明に係る情報再生方法は、情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてユーザデータを復号し、上記認証された情報記録媒体から上記暗号鍵を用いてユーザデータを復号することを特徴とする。

【0016】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【0017】

本発明は、例えば図1に示すような構成の光ディスク1を用いた記録／再生システムに適用される。

【0018】

図1に示した光ディスク1は、情報の記録／再生可能なRAMディスクであり、中心孔2を中心としてそれぞれ環状に形成された3つの情報記録領域であるユーザデータ記録部3、ランダムパターン情報記録部4及び認証データ記録部5を有する。上記ユーザデータ記録部3、ランダムパターン情報記録部4及び認証データ記録部5は、それぞれ独立にアクセスして情報を読み出すことができるように、例えば、2次元的に分離した状態、又は、3次元的に分離した状態に配置される。

【0019】

この光ディスク1では、情報記録領域をディスク半径方向に2次元的に分離することにより、上記ユーザデータ記録部3、ランダムパターン情報記録部4及び認証データ記録部5が形成されている。

【0020】

この光ディスク1において、外周側に形成されたユーザデータ記録部3は、ユーザデータが記録／再生されるデータエリアである。

【0021】

また、内周側に形成されたランダムパターン情報記録部4は、ランダムな物理現象によるランダムパターン情報が記録された読み取り専用の領域である。

【0022】

このランダムパターン情報記録部4は、メディアの製造時に例えば磁気を帯びた細かい繊維を、このランダムパターン情報記録部4の領域にランダムに撒いて固定することにより形成される。このようにして形成されたランダムパターン情報記録部4は、上記磁気を帯びた細かい繊維によるランダムパターン情報が検出可能に記録されたものとなる。

【0023】

なお、上記ランダムパターン情報記録部4は、ランダムにビットを形成し、そのジッターをランダムパターン情報として検出できるようにしてもよい。

【0024】

さらに、上記ランダムパターン情報記録部4の外周側に形成された認証データ

記録部 5 は、上記ランダムパターン情報記録部 4 から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された領域である。この認証データ記録部 5 は、リードインエリアに設けられている。

【0025】

このような構成の光ディスク 1 は、例えば図 2 に示すような構成の認証データ記録装置 10 により、上記認証データ記録部 5 に認証データが記録される。

【0026】

この図 2 に示した認証データ記録装置 10 は、サーボ回路 11 により制御されるスピンドルモータ 12、上記光ディスク 1 の情報記録面を光学的に走査する記録／再生ヘッド 13、上記光ディスク 1 のランダムパターン情報記録部 4 からランダムパターン情報を検出するランダムパターン情報検出部 14、媒体識別情報 r を生成する媒体識別情報生成部 15、認証データを生成する認証データ生成部 16、入力操作部 17 から入力される設定情報に基づいて上記サーボ回路 11 や認証データ生成部 16 を制御する制御部 18 等を備える。

【0027】

上記スピンドルモータ 12 は、サーボ回路 11 による制御に基づいて、上記光ディスク 1 を例えば線速度一定の状態 で回転駆動させる。

【0028】

上記記録／再生ヘッド 13 は、上記スピンドルモータ 12 により回転駆動される光ディスク 1 の認証データ記録部 5 を光学的に走査する光学ヘッドからなり、上記認証データ記録部 5 を介して認証データの記録／再生を行う。

【0029】

上記ランダムパターン情報検出部 14 は、上記スピンドルモータ 12 により回転駆動される光ディスク 1 のランダムパターン情報記録部 4 を走査する磁気ヘッドからなり、上記ランダムパターン情報記録部 4 からランダムパターン情報をアナログ的に検出する。このランダムパターン情報検出部 14 は、上記ランダムパターン情報記録部 4 から検出したランダムパターン情報を上記媒体識別情報生成部 15 に供給する。

【0030】

上記媒体識別情報生成部15は、上記ランダムパターン情報検出部14によりアナログ的に検出されたランダムパターン情報からデジタルのランダムパターン情報に変換し、これを媒体識別情報rとして上記認証データ生成部16に供給する。

【0031】

上記認証データ生成部16は、上記媒体識別情報生成部15から供給される媒体識別情報rに該媒体識別情報rに対する製造者毎のデジタル署名を付して認証データとする。

【0032】

ここで、上記認証データ生成部16により製造者毎のデジタル署名を付した認証データを生成するに当たり、記録媒体の製造者は、信頼できるトラステッド・センター(TC:Trusted Center)を使用し、デジタル署名の検証に必要な自分の公開鍵をTCに登録し、証明書(Cert)を発行してもらっておく。証明書(Cert)は、製造者の識別情報IDや公開鍵などにTCがデジタル署名を施したデータである。

【0033】

また、デジタル署名技術は、あるデータを生成したのがあるユーザであることを証明できる技術であり、例えばIEEE P1363で使用されているElliptic Curve Digital Signature Algorithm(EC-DSA)方式などがよく知られている。

【0034】

この認証データ記録装置10では、上記認証データ生成部16の具体的な処理内容を図3に示してあるように、上記媒体識別情報生成部15から供給される媒体識別情報rに媒体製造日や製造者番号などの付加情報uを付加して、データmを生成する(ステップS1)。このデータmに対し、トラステッド・センターに登録した公開鍵に対応する製造者別の秘密鍵を用いてデジタル署名データsを生成する(ステップS2)。

【0035】

なお、上記付加情報uは、必要に応じて上記媒体識別情報rに付加すればよい

データである。

【0036】

そして、上記認証データ生成部16は、上記データmとデジタル署名データsと証明書(Cert)データをリボケーションリストを合わせて認証データwとし(ステップS3)、この認証データwを上記記録/再生ヘッド13に供給する(ステップS4)ことにより、上記光ディスク1の認証データ記録部5に記録する。

【0037】

ここで、上記付加情報u、製造者別の秘密鍵及び証明書(Cert)データは、例えば上記入力操作部17から上記制御部18に入力されることにより、上記制御部18から上記認証データ生成部16に与えられる。

【0038】

この認証データ記録装置10では、トラステッド・センターから与えられるリボケーションリストを上記入力操作部17から上記制御部18に入力することにより、上記リボケーションリストを上記制御部18から上記認証データ生成部16に与えて、上記光ディスク1の認証データ記録部5に記録することができるようになっている。上記光ディスク1の認証データ記録部5には、トラステッド・センターから与えられる最新版のリボケーションリストを記録する。

【0039】

ここで、リボケーションリストは、単調増加であるそのバージョンナンバーと、秘密鍵が露呈したり不正を働いた判断された製造者の識別情報IDにトラステッド・センターがデジタル署名を施したものである。

【0040】

記録媒体の製造者は、このような構成の認証データ記録装置10により、上記データmとデジタル署名データsと証明書(Cert)データとリボケーションリストを認証データwとして認証データ記録部5に記録した光ディスク1を製造することができる。

【0041】

このような構成の光ディスク1は、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部4から検出されるランダムパタ

ーン情報と、認証データ記録部 16 に記録されている認証データによる認証処理により正当性を検証することができる。上記ランダムパターン情報記録部 4 に記録されているランダムパターン情報は、ランダムな物理現象によるものであるから、複製することはできない。

【0042】

上述の如き構成の光ディスク 1 は、例えば図 4 に示すような構成の光ディスク記録／再生装置 20 により、データの記録／再生が行われる。

【0043】

図 4 に示した光ディスク記録／再生装置 20 は、サーボ回路 21 により制御されるスピンドルモータ 22、上記光ディスク 1 の情報記録面を光学的に走査する記録／再生ヘッド 23、上記光ディスク 1 のランダムパターン情報記録部 4 からランダムパターン情報を検出するランダムパターン情報検出部 24、媒体識別情報検査データ r' を生成する媒体識別情報検査データ生成部 25、認証処理部 26、記録／再生部 27、入力操作部 28 から入力される設定情報に基づいて上記サーボ回路 21 や記録／再生部 27 を制御する制御部 19 等を備える。

【0044】

上記スピンドルモータ 22 は、サーボ回路 21 による制御に基づいて、上記光ディスク 1 を例えば線速度一定の状態 で回転駆動させる。

【0045】

上記記録／再生ヘッド 23 は、上記スピンドルモータ 22 により回転駆動される光ディスク 1 の情報記録面を認証データ記録部 5 を光学的に走査する光学ヘッドからなり、上記認証データ記録部 5 に記録されている認証データの再生や、上記ユーザデータ部 3 に対するデータの記録／再生を行う。

【0046】

上記ランダムパターン情報検出部 24 は、上記スピンドルモータ 22 により回転駆動される光ディスク 1 のランダムパターン情報記録部 4 を走査する磁気ヘッドからなり、上記ランダムパターン情報記録部 4 からランダムパターン情報をアナログ的に検出する。このランダムパターン情報検出部 24 は、上記ランダムパターン情報記録部 4 から検出したランダムパターン情報を上記媒体識別情報検査

データ生成部 25 に供給する。

【0047】

上記媒体識別情報検査データ生成部 25 は、上記ランダムパターン情報検出部 24 によりアナログ的に検出されたランダムパターン情報からデジタルのランダムパターン情報に変換し、これを媒体識別情報検査データ r' として上記認証処理部 26 に供給する。

【0048】

上記認証処理部 26 は、上記光ディスク 1 が正当な製造者により製造されたものであることを認証する処理を行うものである。この認証処理部 26 は、上記記録／再生ヘッド 23 により上記光ディスク 1 の認証データ記録部 5 から再生される認証データ w^{\wedge} が記録／再生部 27 を介して供給されており、上記媒体識別情報生成部 25 から供給される媒体識別情報検査データ r' と上記認証データ w^{\wedge} に基づいて認証処理を行う。

【0049】

上記認証処理部 26 の具体的な処理内容を図 5 に示してある。

【0050】

すなわち、上記認証処理部 26 は、上記媒体識別情報検査データ r' と上記認証データ w^{\wedge} を取り込むと（ステップ S11）、先ず、上記認証データ w^{\wedge} に入っているリボケーションリストの正当性すなわちトラステッド・センターのデジタル署名の正当性をトラステッド・センターの公開鍵を用いて検証する（ステップ S12）。トラステッド・センターの公開鍵は、システム全体で共通であり、機器を製造する際に機器内の不揮発性メモリに格納されている。

【0051】

上記リボケーションリストの検証の結果、リボケーションリストが正当なものであったら、上記リボケーションリストのバージョンナンバーを検証し（ステップ S13）、現在保存しているリボケーションリストと比較しバージョンナンバーが新しい場合には、不揮発性メモリに格納する（ステップ S14）。不揮発性メモリは、図 6 に示すようなリボケーションリストが格納される。

【0052】

次に、上記認証データ w^{\wedge} 中の証明書(Cert)データを取り出し(ステップS15)、上記証明書(Cert)データに含まれる製造者の識別情報IDが上記不揮発性メモリに格納しているリボケーションリストに載っていないことを検証し(ステップS16)、さらに、上記証明書(Cert)データに含まれるトラステッド・センタのデジタル署名が正しいことを検証する(ステップS17)。

【0053】

この検証に合格したら、上記認証データ w^{\wedge} からデータ m^{\wedge} とデジタル署名データ s^{\wedge} を取り出し(ステップS18)、上記認証データ w^{\wedge} 中のデジタル署名データ s^{\wedge} がデータ m^{\wedge} に対する製造者の正しいデジタル署名になっていることを、上記証明書(Cert)データ中の製造者の公開鍵を用いて検証する(ステップS19)。

【0054】

上記検証に合格したら、検証結果J2を合格とする(ステップS20)。

【0055】

次に、上記認証データ w^{\wedge} から媒体識別情報 r^{\wedge} と付加情報 u^{\wedge} を取り出す(ステップS21)。

【0056】

そして、上記認証データ w^{\wedge} から取り出した媒体識別情報 r^{\wedge} と上記媒体識別情報生成部25により生成された媒体識別情報検査データ r' とを比較し、予め定められた誤差内に収まっていることを検証する(ステップS22)。

【0057】

この検証に合格したら、検証結果J1を合格とする(ステップS23)。

【0058】

上記検証結果J1と検証結果J2が共に合格となれば、この記録媒体を正当なものと判断し、上記媒体識別情報 r^{\wedge} を認証済みの媒体識別情報DiscIDとして記録／再生部27に供給する(ステップS24)。

【0059】

ここで、上記不揮発性メモリは、図7に示すような公開鍵リストを格納するよ

うにすることもできる。

【0060】

この場合、公開鍵リストには、製造者の識別情報IDと、その公開鍵、識別情報IDがリボークされているか否かを示すフラグが格納される。さらに、その機器が扱ったことのあるリボケーションリストのうち最新のバージョンのもののバージョンナンバーが格納される。

【0061】

この機器がデータw[^]から、機器が扱ったいずれのものより新しい、正当なりボケーションリストを得た場合、そのリストに挙げられている識別情報IDに対応するリボケーションフラグをYESすなわちリボークとする。

【0062】

もしそれまでその識別情報IDがテーブル上になければ、その項目を新規に作成してフラグをYESとする。

【0063】

逆に、機器が格納していたテーブルにはあったが、最新のリボケーションリストに識別情報IDが含まれていないものについては、フラグをすべてNOすなわちリボークしないとする。そして、最新のバージョンナンバーの項目を更新する。

【0064】

上記認証データw[^]中から取り出した証明書(Cert)データを検証する際には、製造者の識別情報IDをチェックし、その識別情報IDの項目が格納してあるリストにあり、その公開鍵が記録されていて、リボケーションフラグがNOであれば、証明書(Cert)データの検証は不要であり、テーブルに記録されている公開鍵を使用する。

【0065】

識別情報IDの項目がテーブルにあり、フラグがNOであり、公開鍵が記録されていない場合には、証明書(Cert)データを検証して、正しい場合に公開鍵をテーブルに格納する。

【0066】

識別情報IDの項目がテーブルにあり、フラグがYESである場合には、検証J1の結果を不合格とする。

【0067】

識別情報IDの項目がテーブルにない場合には、証明書(Cert)データを検証して、正しい場合に、その識別情報IDに対応する項目を新規に作成して公開鍵を格納する。このときフラグはNOとする。

【0068】

このように公開鍵リストを持つことにより、多くの場合、すなわち、同一の製造者が製造した媒体を使用するが2回目以降になる場合のほとんどで証明書(Cert)データの検証を省くことが可能となる。

【0069】

この光ディスク記録／再生装置20において、上記記録／再生部27は、入力操作部28から入力される制御命令に応じて制御部29により動作モードが切り換えられる。この記録／再生部27は、暗号化処理部30と復号処理部40を備えており、記録モードには、外部から入力されるユーザデータを上記暗号化処理部30により暗号化し、暗号化したユーザデータを上記記録／再生ヘッド23を介して上記光ディスク1のユーザデータ部3に記録し、また、再生モード時には、上記記録／再生ヘッド23により上記光ディスク1のユーザデータ部3から再生される暗号化されたユーザデータを復号処理部40により復号して外部に出力するようになっている。

【0070】

上記暗号化処理部30は、その具体的な構成を図8に示すように、Kem発生モジュール31、乱数発生回路32、Kd暗号化／復号回路33、Ks暗号化回路35やコンテンツデータ暗号化回路36等からなる。

【0071】

上記Kem発生モジュール31は、マスターキーKmを記憶したKmメモリ31Aと、上記Kmメモリ31Aから上記マスターキーKmが与えられるとともに上記認証処理部26から認証済みの媒体識別情報DiscIDが供給されるハッシュ関

数回路 31B とからなる。

【0072】

上記マスターキー K_m は、著作権のライセンスを受ける際に与えられる秘密鍵である。

【0073】

上記ハッシュ関数回路 31B は、 n ビットのマスターキー K_m と m ビットの媒体識別情報 $DiscID$ とを連結して、例えば下位ビットをマスターキー K_m とし上位ビットを媒体識別情報 $DiscID$ とした $n+m$ ビットの連結データ ($DiscID \parallel K_m$) を生成し、生成した連結データ ($DiscID \parallel K_m$) に対して、次の (1) 式に示すように $hash$ 関数 H を適用して、

$$K_{em} = H(DiscID \parallel K_m)$$

イフェクティブマスターキー K_{em} を生成する。そして、上記ハッシュ関数回路 31B は、上記マスターキー K_m と認証済みの媒体識別情報 $DiscID$ から生成したイフェクティブマスターキー K_{em} を K_d 暗号化／復号回路 33 に供給する。

【0074】

ここで、 $A \parallel B$ の \parallel は、データ A とデータ B の連結を意味する。また、 $hash$ 関数は、任意長の入力データに対して、例えば 64 ビット又は 128 ビットなどの固定長のデータを出力する関数であり、 $y (= hash(x))$ を与えられたとき、 x を求めることが困難であり、かつ、 $hash(x_1) = hash(x_2)$ となる x_1 と x_2 との組を求めることも困難となる関数である。一方向 $hash$ 関数の代表的なものとして MD (Message Digest) 5 や SHA (Secure Hash Algorithm) などが知られている。この一方向 $hash$ 関数については、Bruce Schneier 著「Applied Cryptography (Second Edition), Wiley」に詳しく解説されている。

【0075】

また、上記乱数発生回路 32 は、乱数をセクタキー K_{si} とディスクキー K_d として用いる乱数を発生し、セクタキー K_{si} を上記 K_s 暗号化回路 35 とコンテンツデータ暗号化回路 36 に供給するとともに、ディスクキー K_d を上記 K_d 暗号化／復号回路 33 と K_s 暗号化回路 35 に供給する。

【0076】

上記Kd暗号化／復号回路33は、上記乱数発生回路32から供給されるディスクキーKdを上記イフェクティブマスターキーKemで暗号化して暗号化ディスクキーEKdを生成する。このKd暗号化／復号回路33により生成された暗号化ディスクキーEKdは、上記記録／再生ヘッド23を介して上記光ディスク1のリードインエリアに記録される。また、このKd暗号化／復号回路33は、上記記録／再生ヘッド23を介して上記光ディスク1のリードインエリアから再生される暗号化ディスクキーEKdを復号してディスクキーKdを生成する。このKd暗号化／復号回路33により生成されたディスクキーKdは、上記Ks暗号化回路35に供給される。

【0077】

また、上記Ks暗号化回路35は、上記乱数発生回路32から供給されるセクタキーKsiを上記ディスクキーKdで暗号化して暗号化セクタキーEKsを生成する。このKs暗号化回路35により生成された暗号化セクタキーEKsは、上記記録／再生ヘッド23を介して上記光ディスク1のデータエリアに記録される。

【0078】

さらに、上記コンテンツデータ暗号化回路36は、外部からコンテンツデータとして供給されるユーザデータを上記セクタキーKsiで暗号化することにより、暗号化コンテンツデータを生成する。

【0079】

この上記コンテンツデータ暗号化回路36により生成された暗号化コンテンツデータは、上記記録／再生ヘッド23を介して上記光ディスク1のデータエリアに記録される。

【0080】

ここで、上記光ディスク1のデータエリアは、図9に示すように、複数のセクタSi (i=1, 2, ...) からなる。各セクタSi (i=1, 2, ...) は、ヘッダ及びメインデータ部で構成されており、上記セクタキーKsiをディスクキーKdで暗号化した暗号化セクタキーEKsi (i=1, 2, ...) が

ヘッダに格納され、ユーザデータを上記セクタキー K_{si} で暗号化した暗号化コンテンツデータがメインデータ部に格納される。上記 $i = 1, 2, \dots$ はセクタの番号を示している。なお、簡略化のため、一部の図及び説明文中では、セクタ番号を省略する。

【0081】

また、上記復号処理部40は、その具体的な構成を図10に示すように、 K_{em} 発生モジュール41、 EK_d 復号回路43、 EK_s 復号回路45やコンテンツデータ復号回路46等からなる。

【0082】

上記 K_{em} 発生モジュール41は、著作権のライセンスを受ける際に与えられる秘密鍵であるマスターキー K_m を記憶した K_m メモリ41Aと、上記 K_m メモリ41Aにより与えられるマスターキー K_m と上記認証処理部26により与えられる認証済みの媒体識別情報DiscIDから上述の(1)式に示した演算処理によりイフェクティブマスターキー K_{em} を生成するハッシュ関数回路41Bとからなる。上記ハッシュ関数回路41Bは、上記マスターキー K_m と認証済みの媒体識別情報DiscIDから生成したイフェクティブマスターキー K_{em} を EK_d 復号回路43に供給する。

【0083】

なお、この K_{em} 発生モジュール41は、上述の暗号化処理部30の K_{em} 発生モジュール31と同じ構成のものであり、上記 K_{em} 発生モジュール31を兼用するようにしてよい。

【0084】

上記 EK_d 復号回路43は、上記光ディスク1のリードインエリアから上記記録／再生ヘッド23により再生される暗号化ディスクキー EK_d を上記イフェクティブマスターキー K_m で復号してディスクキー K_d を生成し、復号したディスクキー K_d を EK_s 復号回路45に供給する。

【0085】

また、上記 EK_s 復号回路45は、上記光ディスク1のデータエリアから上記記録／再生ヘッド23により再生される暗号化セクタキー EK_s を上記ディスク

キーK_dで復号してセクタキーK_sを生成し、復号したセクタキーK_sをコンテンツデータ復号回路46に供給する。

【0086】

上記コンテンツデータ復号回路46は、上記光ディスク1のデータエリアから上記記録／再生ヘッド23により再生される暗号化コンテンツデータを上記セクタキーK_sで復号する。

【0087】

このような構成の光ディスク記録／再生装置20では、上記入力操作部28から記録命令が入力されることにより制御部29に記録モードが設定されると、上記制御部29は、図11のフローチャートに示すような手順でユーザデータを光ディスク1に記録するように、上記記録／再生部27を制御する。

【0088】

なお、以下の説明では、上記認証処理部26により光ディスク1に対して既に認証処理が行われており、正当なものであると認証された光ディスク1に対してユーザデータを記録するものとする。

【0089】

記録モードでは、上記記録／再生部27の暗号化処理部30が動作状態となっており、上記暗号化処理部30のK_em発生モジュール31は、上記認証処理部26から認証済みの媒体識別情報DiscIDを受け取り（ステップS31）、マスターキーK_mをK_mメモリ31Aから読み出して（ステップS32）、ハッシュ関数回路31Bにより上記媒体識別情報DiscIDとマスターキーK_mからイフェクティブマスターキーK_emを生成する（ステップS33）。

【0090】

次に、上記K_d暗号化／復号回路33は、上記光ディスク1のリードインエリアに暗号化ディスクキーE_K_dが記録されているか否かを判定する（ステップS34）。

【0091】

そして、上記K_d暗号化回路33は、暗号化ディスクキーE_K_dが記録されていない場合には、乱数発生回路32により発生される例えば40ビットの乱数を

ディスクキーK_dとし（ステップS35）、このディスクキーK_dを上記イフェクティブマスターキーK_{em}で暗号化して暗号化ディスクキーEK_dを生成し、この暗号化ディスクキーEK_dを上記光ディスク1のリードインエリアに記録する（ステップS36）。

【0092】

また、上記K_d暗号化回路33は、暗号化ディスクキーEK_dが記録されていた場合には、上記暗号化ディスクキーEK_dを上記イフェクティブマスターキーK_mで復号して、ディスクキーK_dを得る（ステップS37）。

【0093】

次に、上記K_s暗号化回路35は、上記乱数発生回路32により発生される40ビットの乱数をセクタキーK_{si}とし（ステップS38）、このセクタキーK_{si}を上記ディスクキーK_dで暗号化して暗号化セクタキーEK_{si}を生成し、この暗号化セクタキーEK_{si}をセクタヘッドに記録する（ステップS39）。

【0094】

そして、上記コンテンツデータ暗号化回路36は、ユーザデータを上記セクタキーK_{si}で暗号化して暗号化コンテンツデータを生成し、この暗号化コンテンツデータは、メインデータ部に記録する（ステップS40）。

【0095】

さらに、上記コンテンツデータ暗号化回路36は、記録すべきユーザデータをすべて記録したか否かを判定し（ステップS41）、記録すべきユーザデータがある場合には、次のセクタにアクセスし（ステップS42）、上記ステップS38に戻って、上記ステップS38からステップS42の処理を繰り返す行う。

【0096】

このようにしてユーザデータをすべて上記光ディスク1のデータエリアに記録し終えたら、記録モードを終了する。

【0097】

また、この光ディスク記録／再生装置20では、上記入力操作部28から記録命令が入力されることにより制御部29に再生モードが設定されると、上記制御部29は、図12のフローチャートに示すような手順で光ディスク1からユーザ

データを再生するように、上記記録／再生部 27 を制御する。

【0098】

なお、以下の説明では、上記認証処理部 26 により光ディスク 1 に対して既に認証処理が行われており、正当なものであると認証された光ディスク 1 からユーザデータを再生するものとする。

【0099】

再生モードでは、上記記録／再生部 27 の復号処理部 400 が動作状態となっており、上記復号処理部 40 のK e m発生モジュール 41 は、上記認証処理部 26 から認証済みの媒体識別情報DiscIDを受け取り（ステップS51）、マスターキーK mをK mメモリ 41 Aから読み出して（ステップS52）、ハッシュ関数回路 41 Bにより上記媒体識別情報DiscIDとマスターキーK mからイフェクティブマスターキーK e mを生成する（ステップS53）。

【0100】

次に、上記E K d暗号化／復号回路 33 は、上記光ディスク 1 のリードインエリアから再生される暗号化ディスクキーE K dを上記イフェクティブマスターキーK e mで復号して、ディスクキーK dを生成する（ステップS54）。

【0101】

次に、上記E K s復号回路 35 は、上記光ディスク 1 のデータエリアから再生される暗号化セクタキーE K s iを復号して、セクタキーK s iを生成する（ステップS55）。

【0102】

そして、上記コンテンツデータ復号回路 46 は、上記光ディスク 1 のデータエリアから再生される暗号化コンテンツデータを上記セクタキーK sで復号する（ステップS56）。

【0103】

さらに、上記コンテンツデータ復号回路 46 は、再生すべきコンテンツデータをすべて再生したか否かを判定し（ステップS57）、再生すべきコンテンツデータがある場合には、次のセクタにアクセスし（ステップS58）、上記ステップS25に戻って、上記ステップS55からステップS58の処理を繰り返す行

う。

【0104】

このようにして必要なコンテンツデータをすべて上記光ディスク1のデータエリアに再生し終えたら、再生モードを終了する。

【0105】

この光ディスク記録／再生装置20によりユーザデータ記録部3にユーザデータが記録された光ディスク1は、上記ユーザデータの暗号鍵すなわちセクタキーKsが上記ディスクキーKdで暗号化した暗号化セクタキーEKsとしてデータエリアに記録され、さらに、上記ディスクキーKdが、この光ディスク1に固有の媒体識別情報DiscIDに基づいて生成されたイフェクティブマスターキーKemで暗号化した暗号化ディスクキーEKdとしてリードインエリアに記録されているので、上記光ディスク1のランダムパターン情報記録部4に記録されているランダムパターン情報に基づいて生成される媒体識別情報検査データと認証データ記録部5に記録された認証データに基づいて上記媒体識別情報DiscIDについて認証処理を行う認証処理機能を有する正規の再生装置でのみ再生することができ、上記認証処理機能にない再生装置ではユーザデータを復号して再生することはできない。

【0106】

また、仮に、上記光ディスク1のデータエリア及びリードインエリアのデータをそのまま新しいディスクに不正コピーされた場合としても、上記光ディスク1のランダムパターン情報記録部4に記録されているランダムパターン情報はランダムな物理現象によるものであるから、上記新しいディスクがランダムパターン情報記録部を有する正規のものであったとしても、新しいディスクのランダムパターン情報記録部から上記光ディスク1のランダムパターン情報記録部4に記録されているランダムパターン情報と同じランダムパターン情報を検出することはできない。したがって、不正コピーされたディスクが正規の再生装置により再生されることはない。

【0107】

ここで、上述の光ディスク記録／再生装置20では、暗号化処理処理部30に

において、上記認証処理部 26 により認証された光ディスク 1 の媒体識別情報 Disc ID に基づいて、マスターキー K_m からイフェクティブマスターキー K_{em} を生成し、このイフェクティブマスターキー K_{em} でディスクキー K_d を暗号化し、上記ユーザデータの暗号化に用いる暗号鍵すなわちセクターキー K_s を上記ディスクキー K_d で暗号化し、上記セクターキー K_s により暗号化したユーザデータと上記暗号化したディスクキー K_d 及びセクターキー K_s を上記光ディスク 1 に記録するようにしたが、上記認証処理部 26 により認証された光ディスク 1 の媒体識別情報 Disc ID に基づいて、上記ユーザデータを暗号化するようにしてもよい。例えば、例えば図 13 に示すように、上記乱数発生回路 32 で乱数として発生されるセクターキー K_s から上記イフェクティブマスターキー K_{em} に基づいてイフェクティブセクターキー K_{es} を生成するセクターキー生成部 130 を設け、上記コンテンツデータ暗号化回路 35 において、上記セクターキー生成回路 130 により生成されたイフェクティブセクターキー K_{es} でユーザデータを暗号化して暗号化コンテンツデータを生成する。

【0108】

この場合、復号処理部 40 には、図 14 に示すように、イフェクティブマスターキー K_{em} に基づいてセクタキー K_s からイフェクティブセクタキー K_{es} を生成する K_{es} 生成回路 140 を設け、上記光ディスク 1 のデータエリアから上記記録／再生ヘッド 23 により再生される暗号化セクタキー EK_s を上記 EK_s 復号回路 45 により上記ディスクキー K_d で復号してセクターキー K_s を生成し、このセクターキー K_s から上記 K_{es} 生成回路 140 によりイフェクティブセクタキー K_{es} を生成して、このイフェクティブセクタキー K_{es} を用いてコンテンツデータ復号回路 46 により暗号化コンテンツデータを復号する。

【0109】

また、上述の実施の形態では、図 1 に示すような構成の光ディスク 1 を用いた記録／再生システムに本発明を適用したが、図 15 に示すようなカード状記録媒体 51 を用いた記録／再生システムを構築するようにしてもよい。

【0110】

すなわち、この図 13 に示したカード状記録媒体 51 は、ユーザデータが記録

されるユーザデータ記録部 53 と、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部 54 と、上記ランダムパターン情報記録部 54 から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部 55 とを有する。

【0111】

このような構成のカード状記録媒体 51 を使用する記録／再生システムでは、上述の光ディスク記録／再生システムと同様に、上記ランダムパターン情報記録部 54 からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成するとともに、上記情報記録媒体上の認証データ記録部 55 から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報と上記認証データに基づいて上記情報記録媒体に対する認証処理を行うことができ、上記認証処理により認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化したデータを上記認証された情報記録媒体上のユーザデータ記録部 53 を介して記録／再生することにより、上記ユーザデータ記録部 53 の情報の不正コピーを確実に防止することが可能となる。

【0112】

【発明の効果】

以上詳細に説明したように、本発明によれば、情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することによって、媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして認証データ記録部に記録した情報記録媒体を提供することができる。そして、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出

されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証データとして格納した認証データ記録部と、ユーザデータが記録されるユーザデータ記録部とを有する情報記録媒体に対して、上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報と上記認証データに基づいて上記情報記録媒体に対する認証処理を行うことができ、上記認証処理により認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化したデータを上記認証された情報記録媒体上のユーザデータ記録部を介して記録／再生することにより、RAMメディアに対しても有効な不正コピー防止システムを構築することができる。

【図面の簡単な説明】

【図 1】

本発明を適用した光ディスクを説明するための図である。

【図 2】

上記光ディスクに認証データを記録する認証データ記録装置の構成を示すブロック図である。

【図 3】

上記認証データ記録装置における認証データ生成部の具体的な処理内容を示すフローチャートである。

【図 4】

上記光ディスクを使用する光ディスク記録／再生装置の構成を示すブロック図である。

【図 5】

上記光ディスク記録／再生装置における認証処理部の具体的な処理内容を示すフローチャートである。

【図 6】

上記認証処理部による認証処理に使用されるリボケーションリストを示す図で

ある。

【図 7】

上記認証処理部による認証処理に使用される公開鍵リストを示す図である。

【図 8】

上記光ディスク記録／再生装置における記録／再生回路の暗号化処理部の構成を示すブロック図である。

【図 9】

上記光ディスク記録／再生装置により光ディスクに記録されるデータの構造を模式的に示す図である。

【図 10】

上記光ディスク記録／再生装置における記録／再生回路の復号処理部の構成を示すブロック図である。

【図 11】

上記光ディスク記録／再生装置の記録モードの動作を示すフローチャートである。

【図 12】

上記光ディスク記録／再生装置の再生モードの動作を示すフローチャートである。

【図 13】

上記光ディスク記録／再生装置における記録／再生回路の暗号化処理部の他の構成例を示すブロック図である。

【図 14】

上記光ディスク記録／再生装置における記録／再生回路の復号処理部の他の構成例を示すブロック図である。

【図 15】

本発明を適用したカード状情報記録媒体を説明するための図である。

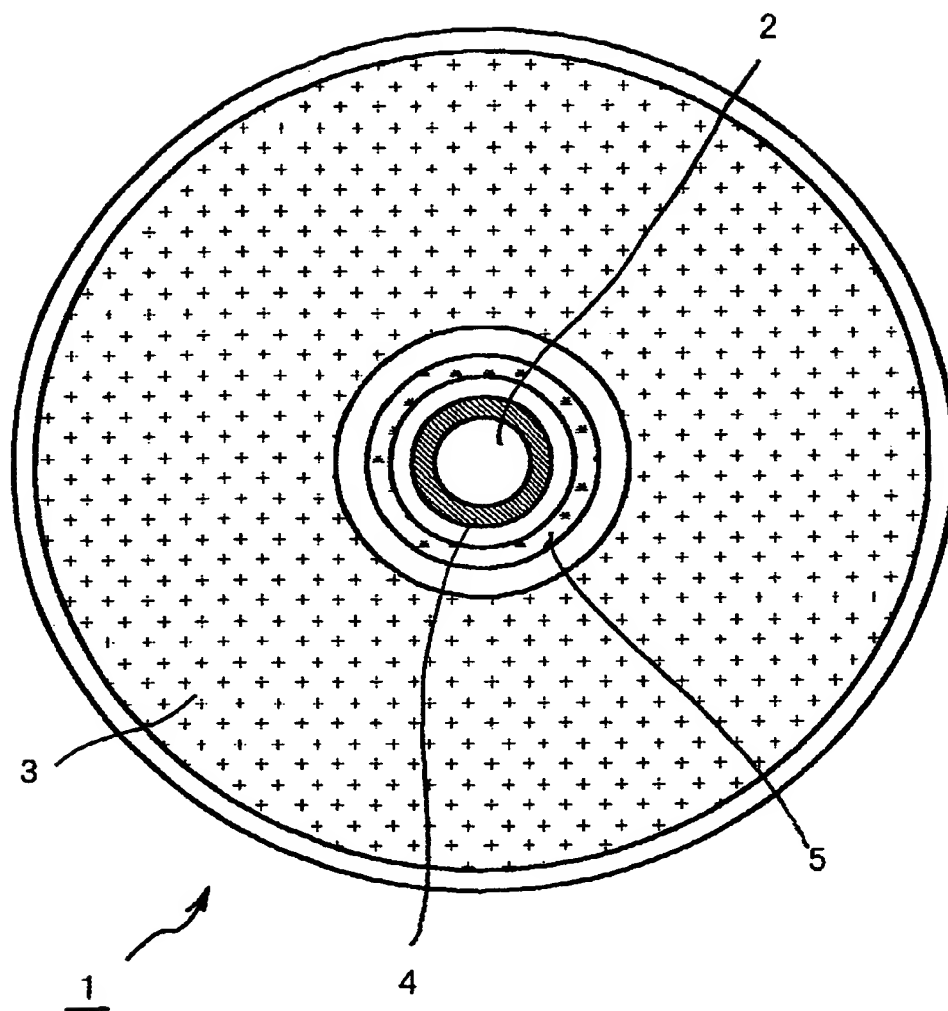
【符号の説明】

1 光ディスク、3, 53 ユーザデータ記録部、4, 54 ランダムパターン情報記録部、5, 55 認証データ記録部、10 認証データ記録装置、13

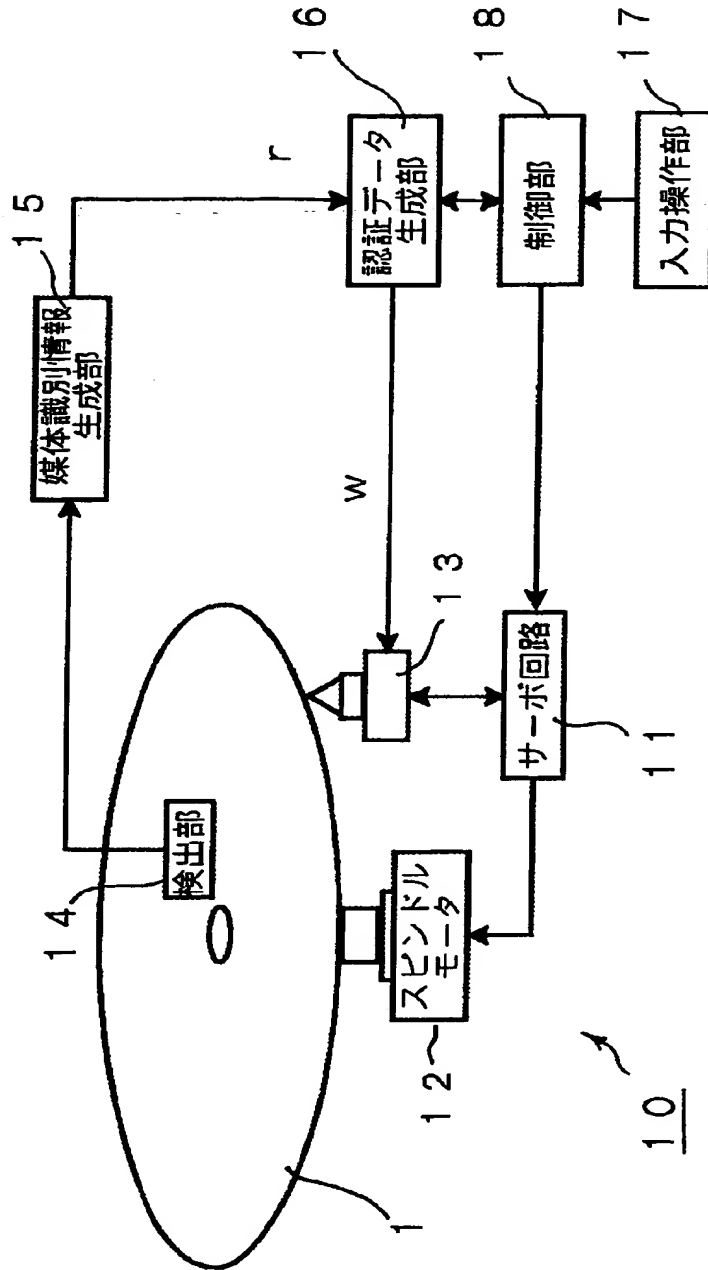
， 23 記録／再生ヘッド、 14， 24 ランダムパターン情報検出部、 15，
25 媒体識別情報生成部、 16 認証データ生成部、 20 光ディスク記録／
再生装置、 30 暗号化処理部、 40 復号処理部、 130、 140 K e s 生成
回路

【書類名】 図面

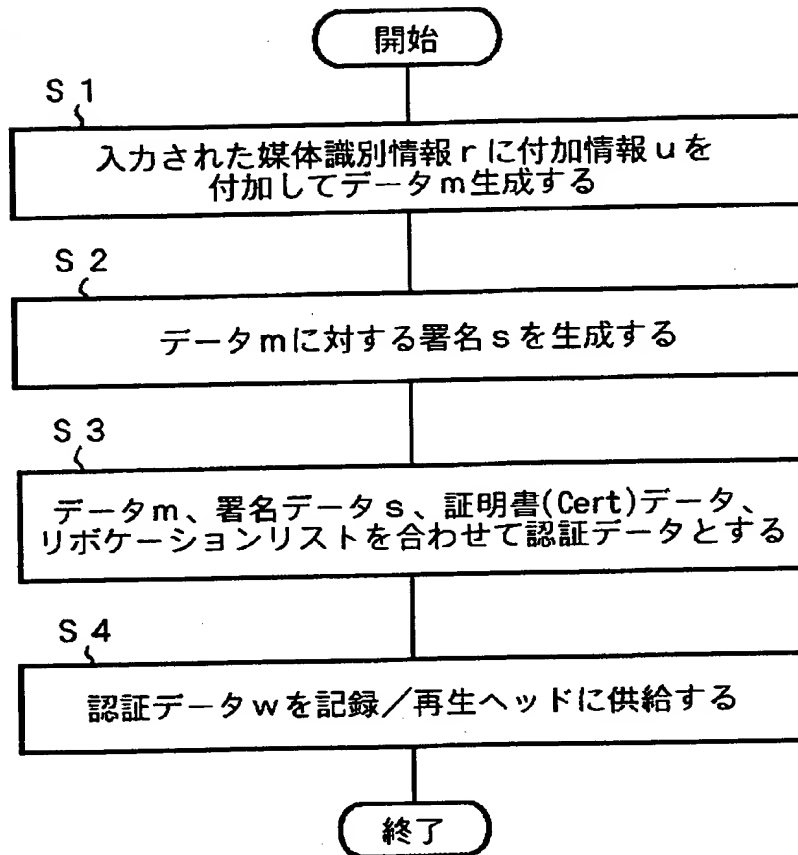
【図 1】



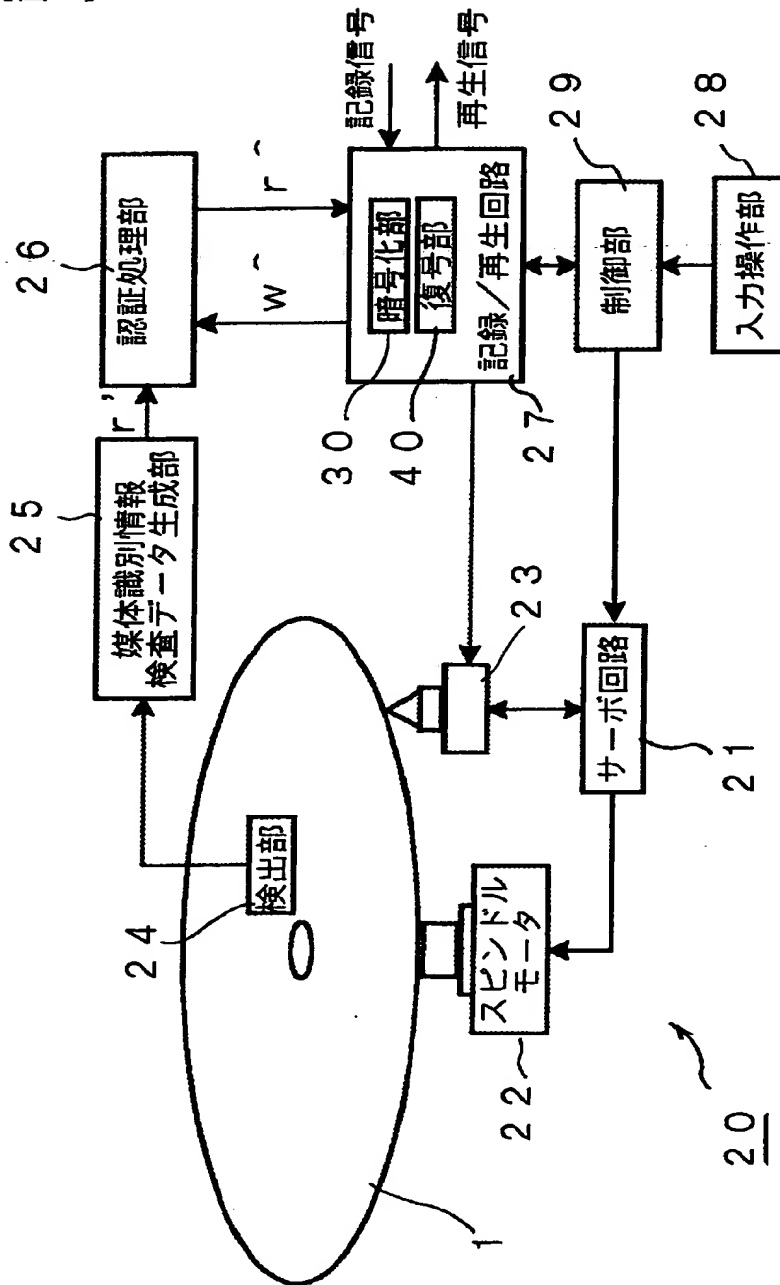
【図 2】



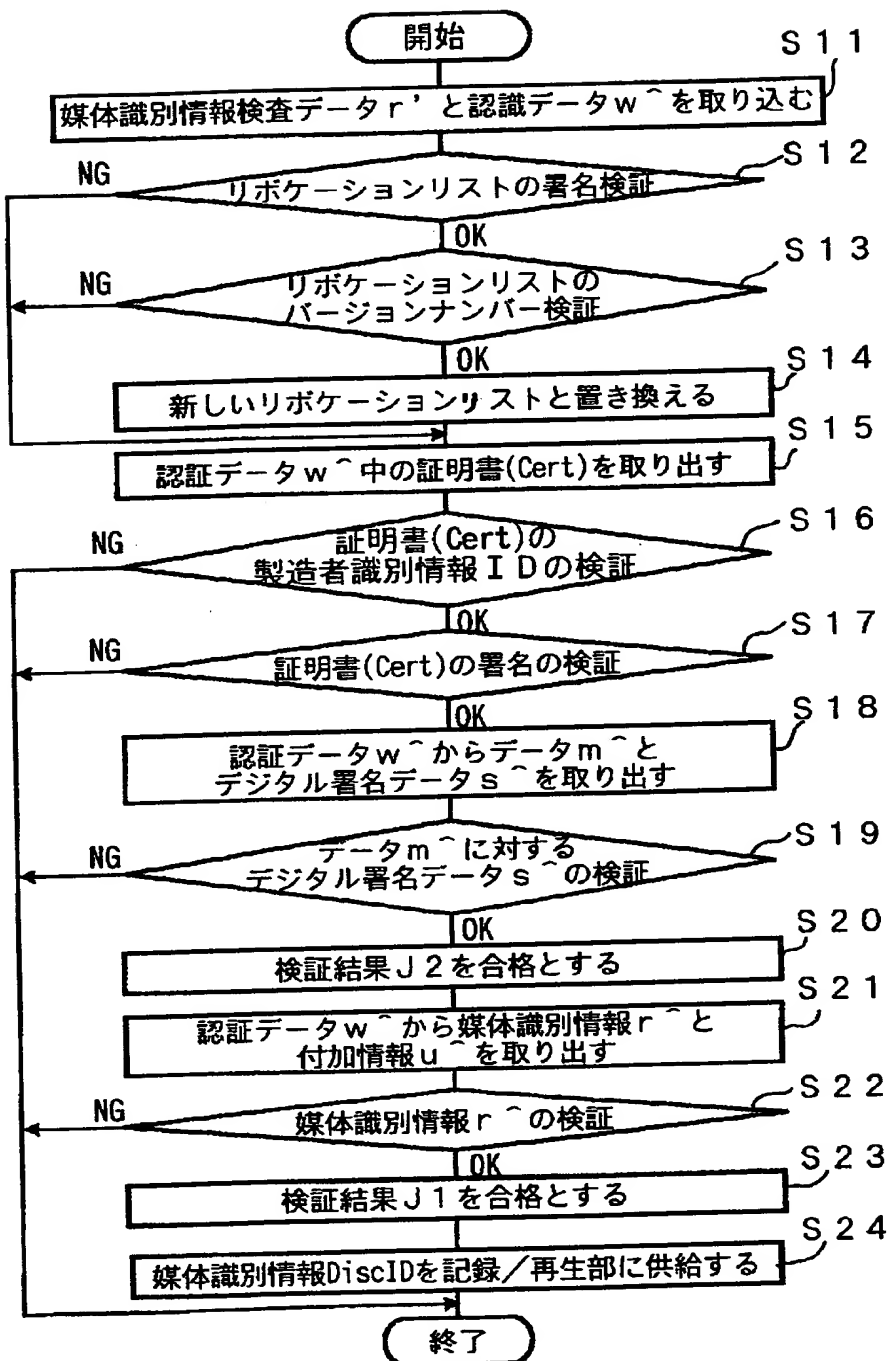
【図 3】



【図 4】



【図 5】



【図 6】

リボケーションリスト

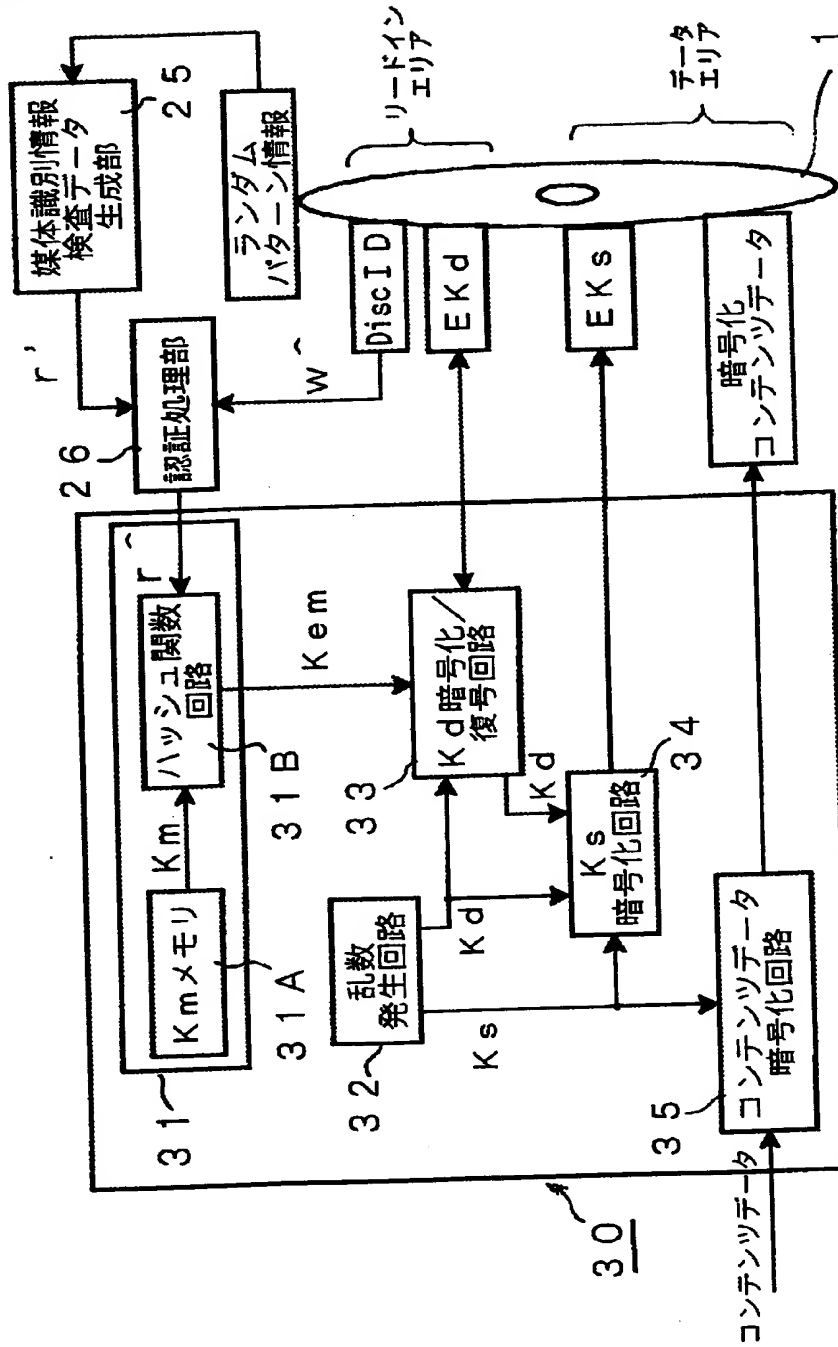
バージョンナンバー
製造者 I D
...

【図 7】

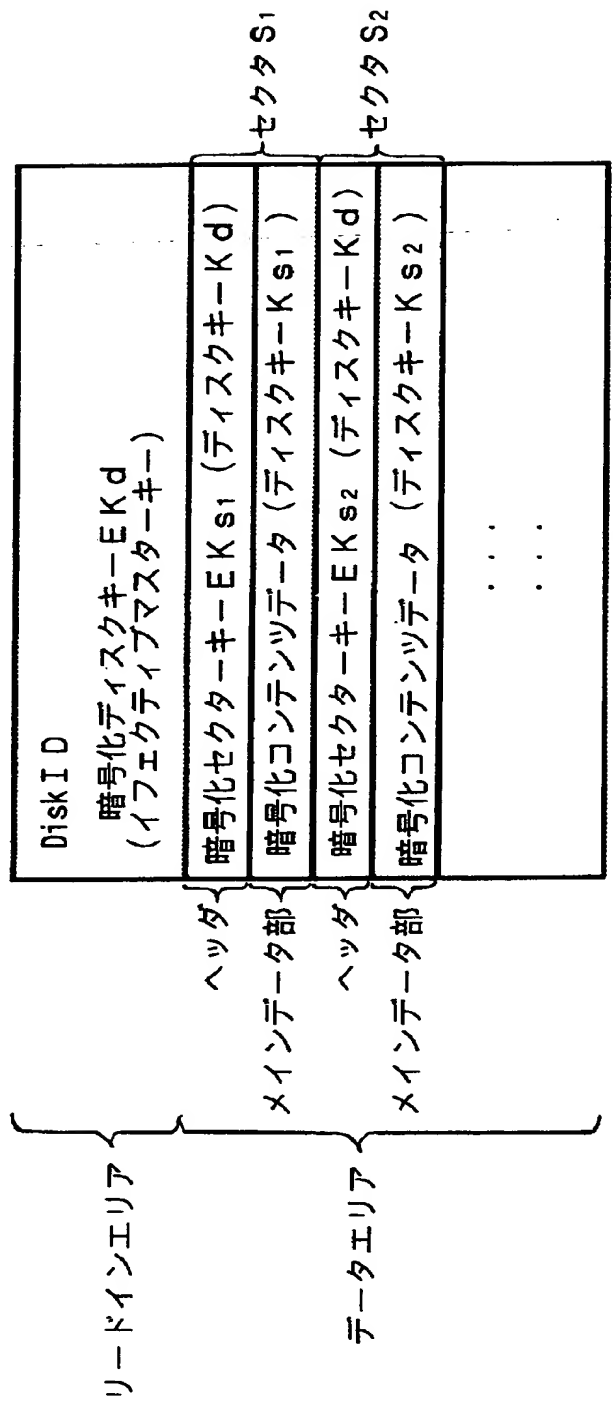
公開鍵リスト

最新のリボケーションリストのバージョンナンバー		
製造者 I D	公開鍵	リボケーションフラグ(YES/NO)
...

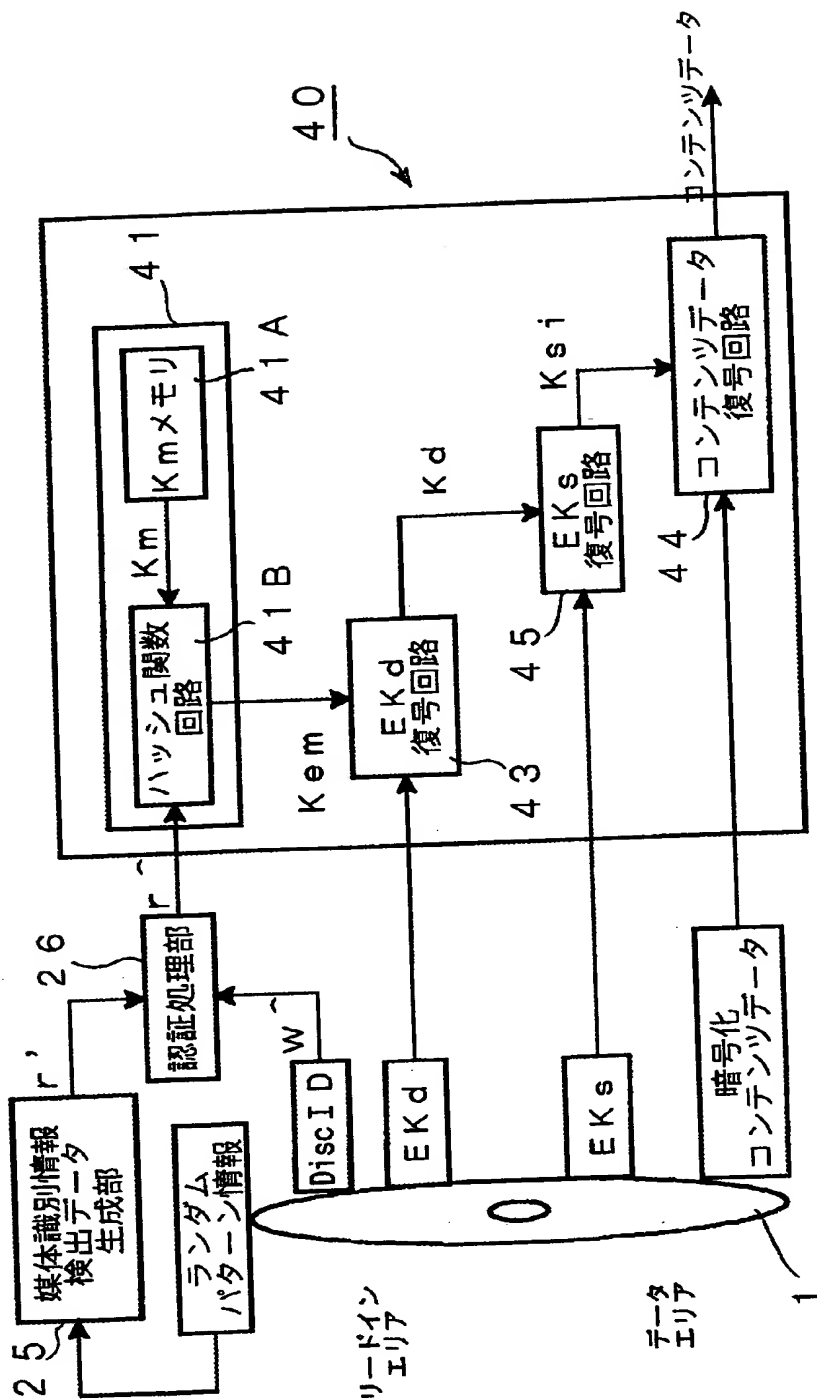
【図 8】



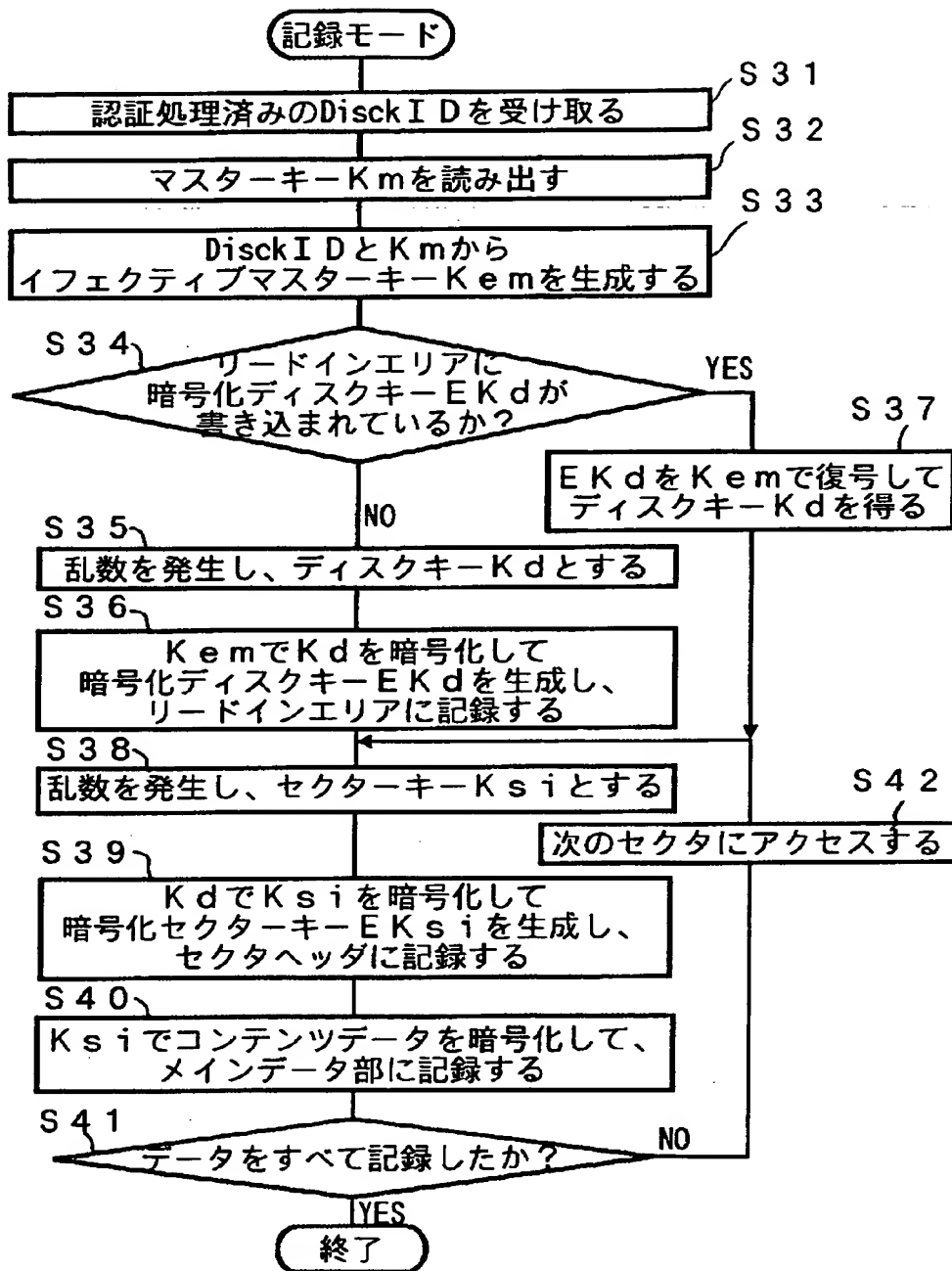
【図 9】



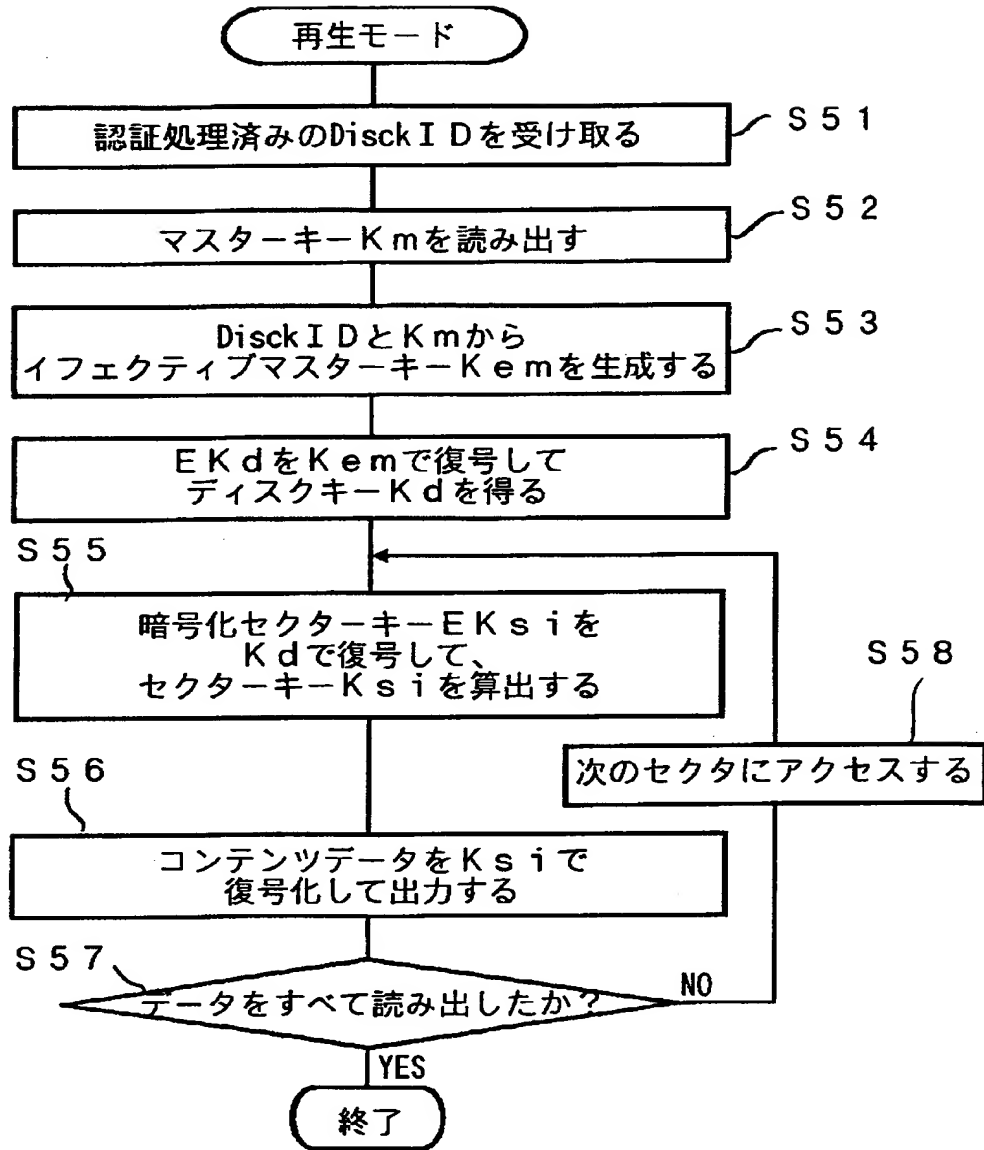
【図 10】



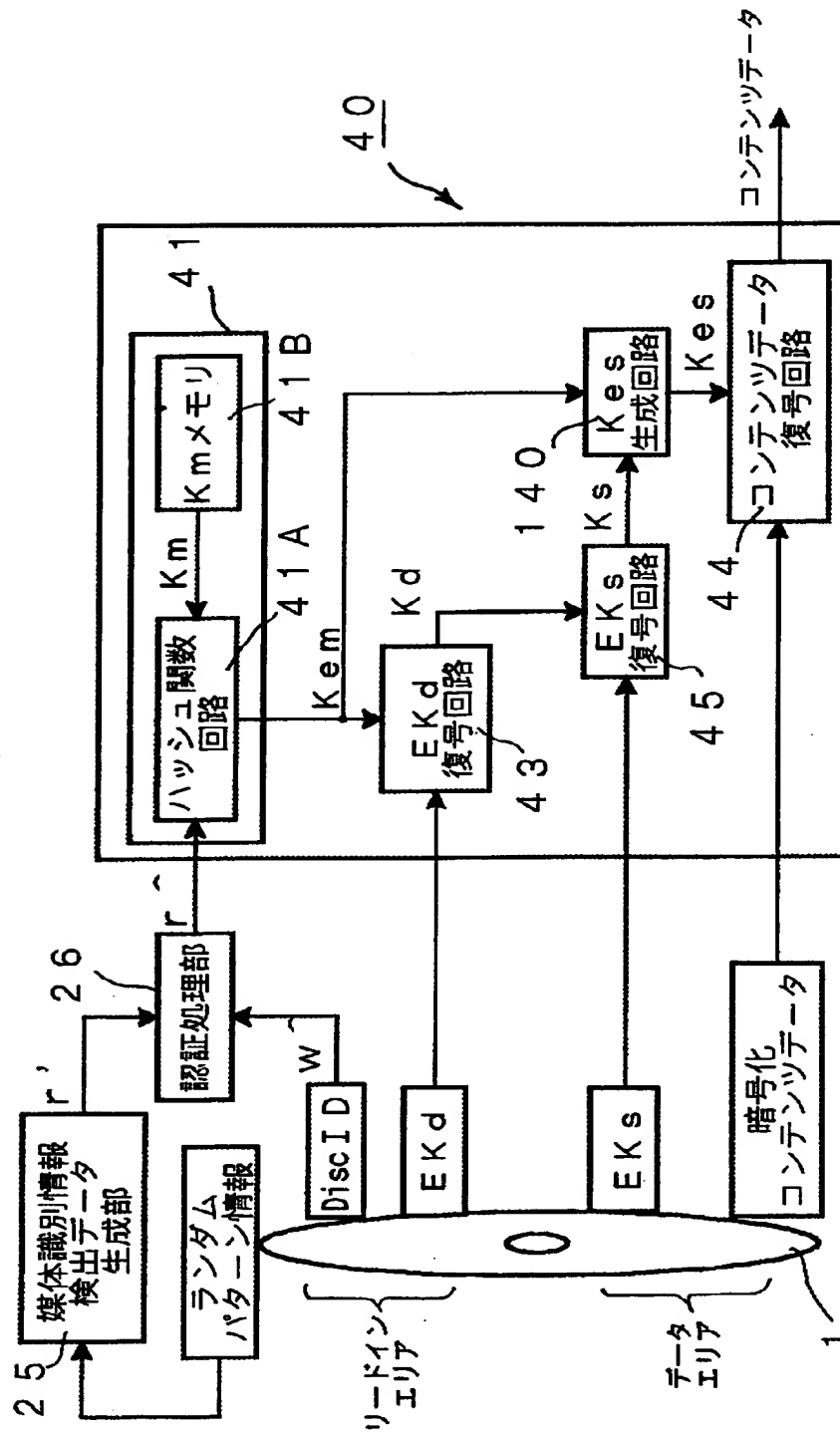
【図 11】



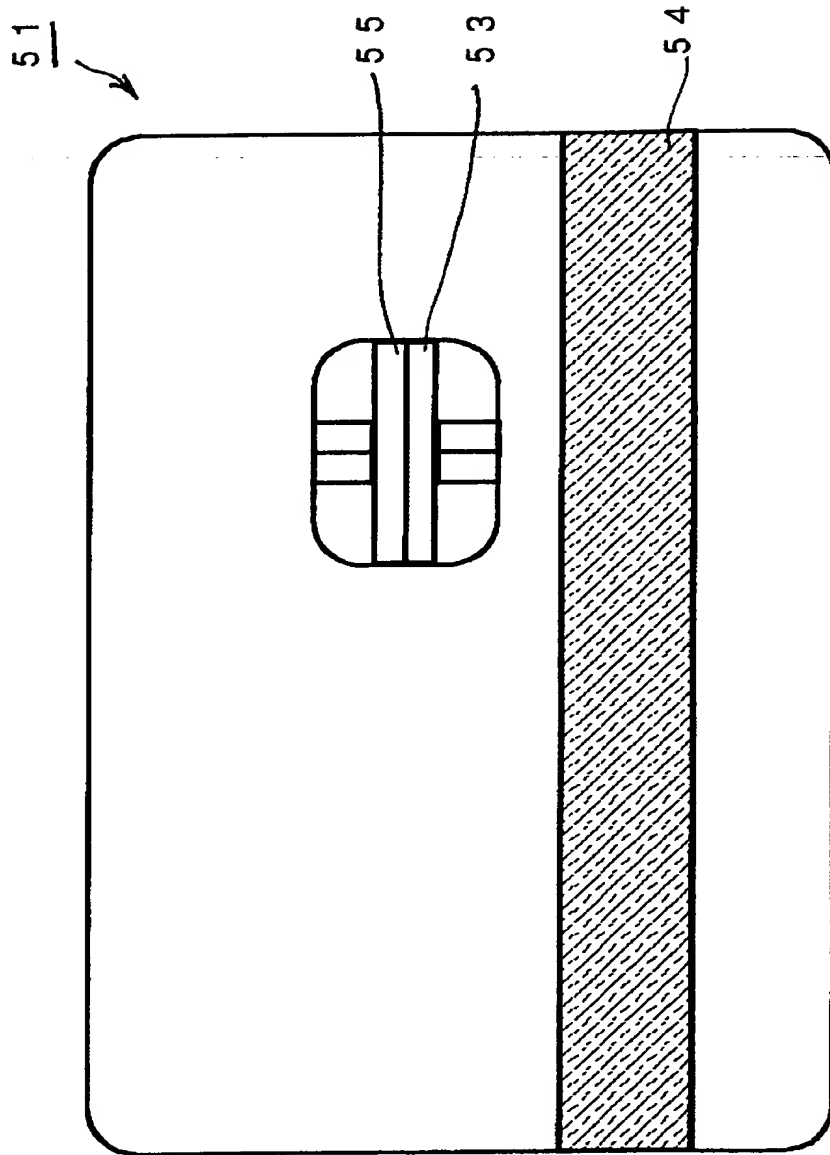
【図 12】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 RAMメディアに対しても有効な不正コピー防止システムを構築する

【解決手段】 情報記録媒体上に、ユーザデータが記録されるユーザデータ記録部3と、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部4と、上記ランダムパターン情報記録部4から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部5とを設ける。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社

This Page Blank (uspto)